

Appln No. 09/690,796
Amdt date December 12, 2007
Reply to Office action of September 20, 2007

REMARKS/ARGUMENTS

Claims 1, 5-10, 17, 22, 42, 50-52, and 55-59 are currently pending. Claims 1, 6, 7, 17, 22, 50-52, and 55-57 are amended.

Applicant thanks the Examiner for his time for the telephonic interviews conducted on November 27 and December 4, 2007.

Claims 1, 6-10, 17, 22, 42, 50-52, and 55-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Lewis et al. (US 6,233,565). Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis et al. in view of Bosen et al. (US 5,060,263). Applicant respectfully submits that all of the pending claims are patentable over the cited references.

Independent claim 1 includes, among other limitations, "a plurality of stateless cryptographic devices, each of the plurality of stateless cryptographic devices configured to perform authentication, processing value for the VBI, and generation of indicia data for the plurality of users, wherein before each of the authentication, processing value, and generation of indicia data for a given user is performed, an available cryptographic device in the server system retrieves the data record for the given user directly from the database." Lewis does not disclose the above limitation.

First, there is no teaching that the cryptographic "modules" of Lewis are stateless. Rather, in the system of Lewis "each client 2n has a cryptographic module 12n and the RSP server 4 has a cryptographic module 14. The server cryptographic module 14 serves three functions: (1) authentication, (2) encryption, and (3) authorization. Authentication is the only function that requires interaction with a client cryptographic module 12." (Col. 21, lines 12-17, underlining is added.). Furthermore, the "main function of the client cryptographic module 12 is to protect the [respective]customer's private key from both intrusion and corruption. The customer's private key is used to authenticate the client 2 to the server 4." (Col. 22, lines 6-8, emphasis is added.). Therefore, Lewis has one (central) server cryptographic module 14, and many client cryptographic modules 12, one for each client and dedicated to that client.

Consequently, "each of" the client cryptographic modules 12 is not capable of authenticating, processing value for the VBI, and generating indicia data for the plurality of users," rather, at least some these are the functions of the only (one central) server cryptographic module 14.

Additionally, Lewis's system does not disclose "an available cryptographic device retrieves the data record for the given user directly from the database," because, as explained above, Lewis's system has one client cryptographic modules 12 for each client and dedicated to that client. Therefore, a client cryptographic module 12j cannot "retrieve the data record" for a user-k, even though the client cryptographic module 12j may be available.

Furthermore, Lewis makes it clear that "all sensitive data is stored in a Secure SQL Server Database and protected by SQL Integrated NT security. See FIG. 3. The Secure SQL Server database 305 is considered a part of the server cryptographic 14 module and may only be accessed by the cryptographic module [14]." (Col. 25, lines 55-59, emphasis is added.). Therefore, the client cryptographic modules 12 cannot "retrieve the data record for the given user directly from the database."

As a result, claim 1 is not anticipated by Lewis.

Independent claim 50 includes, among other limitations, "directly retrieving the data record for a given user from the database for authenticating the given user, processing value for the VBI and generating indicia data for the given user, by any available cryptographic device of the plurality of stateless cryptographic devices." Likewise, Lewis does not teach the above limitation.

First, as explained above, Lewis does not teach a plurality of stateless cryptographic devices. Second, as explained above, the plurality of client cryptographic modules 12 of Lewis cannot authenticate the given user, process value for the VBI and generate indicia data for the given user rather, at least some of these are the functions of the only (one central) server cryptographic module 14. Third, Lewis's system does not disclose "an available cryptographic device retrieves the data record for the given user directly from the database," because, as

Appln No. 09/690,796
Amdt date December 12, 2007
Reply to Office action of September 20, 2007


explained above, Lewis's system has one client cryptographic modules 12 for each client and dedicated to that client.

Fourth, client cryptographic modules 12 of Lewis cannot "retrieve the data record for the given user directly from the database," because "database 305 is considered a part of the server cryptographic 14 module and may only be accessed by the cryptographic module [14]." (Id.).

In short, independent claims 1, and 50 define a novel and unobvious invention over the cited references. Dependent claims 5-10, 17, 22, 42, 51, 52, and 55-59 are dependent from claims 1 and 50, respectively and therefore include all the limitations of their respective independent claims and additional limitations therein. Accordingly, these claims are also allowable over the cited references, as being dependent from allowable independent claims and for the additional limitations they include therein.

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By 
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv

CLV PAS768860.1-*12/12/07 10:16 AM